

# VU Research Portal

## Split-2 bisimilarity has a finite axiomatization over CCS with Hennessy's merge

Aceto, L.; Fokkink, W.J.; Ingólfssdóttir, A.; Luttik, B.

### **published in**

Logical Methods in Computer Science  
2005

### **DOI (link to publisher)**

[10.2168/lmcs-1\(1:3\)2005](https://doi.org/10.2168/lmcs-1(1:3)2005)

### **document version**

Publisher's PDF, also known as Version of record

[Link to publication in VU Research Portal](#)

### **citation for published version (APA)**

Aceto, L., Fokkink, W. J., Ingólfssdóttir, A., & Luttik, B. (2005). Split-2 bisimilarity has a finite axiomatization over CCS with Hennessy's merge. *Logical Methods in Computer Science*, 1(1). [https://doi.org/10.2168/lmcs-1\(1:3\)2005](https://doi.org/10.2168/lmcs-1(1:3)2005)

### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

### **Take down policy**

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

### **E-mail address:**

[vuresearchportal.ub@vu.nl](mailto:vuresearchportal.ub@vu.nl)

## SPLIT-2 BISIMILARITY HAS A FINITE AXIOMATIZATION OVER CCS WITH HENNESSY’S MERGE

LUCA ACETO <sup>a</sup>, WAN FOKKINK <sup>b</sup>, ANNA INGOLFSDOTTIR <sup>c</sup>, AND BAS LUTTIK <sup>d</sup>

<sup>a</sup> BRICS, Department of Computer Science, Aalborg University, 9220 Aalborg Ø, Denmark, and  
School of Computer Science, Reykjavík University, Iceland  
*e-mail address*: luca@cs.aau.dk, luca@ru.is

<sup>b</sup> Vrije Universiteit Amsterdam, Department of Computer Science, Section Theoretical Computer  
Science, De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands  
*e-mail address*: wanf@cs.vu.nl

<sup>c</sup> BRICS, Department of Computer Science, Aalborg University, 9220 Aalborg Ø, Denmark, and  
Department of Computer Science, University of Iceland, Iceland  
*e-mail address*: annai@cs.aau.dk, annaing@hi.is

<sup>d</sup> Department of Mathematics and Computer Science, Eindhoven Technical University, 5600 MB Eind-  
hoven, The Netherlands  
*e-mail address*: luttik@win.tue.nl

---

**ABSTRACT.** This note shows that split-2 bisimulation equivalence (also known as timed equivalence) affords a finite equational axiomatization over the process algebra obtained by adding an auxiliary operation proposed by Hennessy in 1981 to the recursion, relabelling and restriction free fragment of Milner’s Calculus of Communicating Systems. Thus the addition of a single binary operation, viz. Hennessy’s merge, is sufficient for the finite equational axiomatization of parallel composition modulo this non-interleaving equivalence. This result is in sharp contrast to a theorem previously obtained by the same authors to the effect that the same language is not finitely based modulo bisimulation equivalence.

### 1. INTRODUCTION

This note offers a contribution to the study of equational characterizations of the parallel composition operation modulo (variations on) the classic notion of bisimulation equivalence [Mil89, Par81]. In particular, we provide a finite equational axiomatization of *split-2 bisimulation equivalence*—a notion of bisimulation equivalence based on the assumption that actions have observable beginnings and endings [GV87, GL95, Hen88]—over the recursion, relabelling and restriction free fragment of Milner’s CCS [Mil89] enriched with an auxiliary operator proposed by Hennessy in a 1981 preprint entitled “*On the relationship between*

---

*2000 ACM Subject Classification:* D.3.1, F.1.1, F.1.2, F.3.2, F.3.4, F.4.1.

*Key words and phrases:* Concurrency, process algebra, CCS, bisimulation, split-2 bisimulation, non-interleaving equivalences, Hennessy’s merge, left merge, communication merge, parallel composition, equational logic, complete axiomatizations, finitely based algebras.

*time and interleaving*” and its published version [Hen88]. To put this contribution, and its significance, in its research context, we find it appropriate to recall briefly some of the key results in the history of the study of equational axiomatizations of parallel composition in process algebra.

Research on equational axiomatizations of behavioural equivalences over process algebras incorporating a notion of parallel composition can be traced at least as far back as the seminal paper [HM85], where Hennessy and Milner offered, amongst a wealth of other classic results, a complete equational axiomatization of bisimulation equivalence over the recursion free fragment of CCS. (See the paper [Bae04] for a more detailed historical account highlighting, e.g., Hans Bekić’s early contributions to this field of research.) The axiomatization given by Hennessy and Milner in that paper dealt with parallel composition using the so-called *expansion law*—an axiom schema with a countably infinite number of instances that is essentially an equational formulation of the Plotkin-style rules describing the operational semantics of parallel composition. This raised the question of whether the parallel composition operator could be axiomatized in bisimulation semantics by means of a finite collection of equations. This question was answered positively by Bergstra and Klop, who gave in [BK84] a finite equational axiomatization of the merge operator in terms of the auxiliary left merge and communication merge operators. Moller clarified the key role played by the expansion law in the axiomatization of parallel composition over CCS by showing in [Mol89, Mol90a, Mol90b] that strong bisimulation equivalence is *not* finitely based over CCS and PA without the left merge operator. (The process algebra PA [BK84] contains a parallel composition operator based on pure interleaving without communication and the left merge operator.) Thus auxiliary operators like the ones used by Bergstra and Klop are indeed necessary to obtain a finite axiomatization of parallel composition. Moreover, Moller proved in [Mol89, Mol90a] that his negative result holds true for each “reasonable congruence” that is included in standard bisimulation equivalence. In particular, this theorem of Moller’s applies to split-2 bisimulation equivalence since that equivalence is “reasonable” in Moller’s technical sense.

In his paper [Hen88], Hennessy proposed an axiomatization of observation congruence [HM85] (also known as rooted weak bisimulation equivalence) and timed congruence (essentially rooted weak split-2 bisimulation equivalence) over a CCS-like recursion, relabelling and restriction free process language. Those axiomatizations used an auxiliary operator, denoted  $\mid$  by Hennessy, that is essentially a combination of Bergstra and Klop’s left and communication merge operators. Apart from having soundness problems (see the reference [Ace94] for a general discussion of this problem, and corrected proofs of Hennessy’s results), the proposed axiomatization of observation congruence is *infinite*, as it used a variant of the expansion theorem from [HM85]. Confirming a conjecture by Bergstra and Klop in [BK84, page 118], and answering problem 8 in [Ace03], we showed in [AFIL03] that the language obtained by adding Hennessy’s merge to CCS does *not* afford a finite equational axiomatization modulo bisimulation equivalence. This is due to the fact that, in strong bisimulation semantics, no finite collection of equations can express the interplay between interleaving and communication that underlies the semantics of Hennessy’s merge. Technically, this is captured in our proof of the main result in [AFIL03] by showing that no finite collection of axioms that are valid in bisimulation semantics can prove all of the

equations in the following family:

$$a\mathbf{0} \not\sim \sum_{i=0}^n \bar{a}a^i \approx a \sum_{i=0}^n \bar{a}a^i + \sum_{i=0}^n \tau a^i \quad (n \geq 0) .$$

In split-2 semantics, however, these equations are not sound, since they express some form of interleaving. Indeed, we prove that, in sharp contrast to the situation in standard bisimulation semantics, the language with Hennessy's merge *can be finitely axiomatized* modulo split-2 bisimulation equivalence, and its use suffices to yield a finite axiomatization of the parallel composition operation. This shows that, in contrast to the results offered in [Mol89, Mol90a], “reasonable congruences” finer than standard bisimulation equivalence can be finitely axiomatized over CCS using Hennessy's merge as the single auxiliary operation—compare with the non-finite axiomatizability results for these congruences offered in [Mol89, Mol90a].

The paper is organized as follows. We begin by presenting preliminaries on the language  $\text{CCS}_H$ —the extension of CCS with Hennessy's merge operator—and split-2 bisimulation equivalence in Sect. 2. We then offer a finite equational axiom system for split-2 bisimulation equivalence over  $\text{CCS}_H$ , and prove that it is sound and complete (Sect. 3).

This is a companion paper to [AFIL03], where the interested readers may find further motivation and more references to related literature. However, we have striven to make it readable independently of that paper. Some familiarity with [Ace94, Hen88] and the basic notions on process algebras and bisimulation equivalence will be helpful, but is not necessary, in reading this study. The uninitiated reader is referred to the textbooks [BW90, Mil89] for extensive motivation and background on process algebras. Precise pointers to material in [Ace94, Hen88] will be given whenever necessary.

## 2. THE LANGUAGE $\text{CCS}_H$

The language for processes we shall consider in this paper, henceforth referred to as  $\text{CCS}_H$ , is obtained by adding Hennessy's merge operator from [Hen88] to the recursion, restriction and relabelling free subset of Milner's CCS [Mil89]. This language is given by the following grammar:

$$p ::= \mathbf{0} \mid \mu p \mid p + p \mid p \mid p \mid p \not\sim p ,$$

where  $\mu$  ranges over a set of *actions*  $A$ . We assume that  $A$  has the form  $\{\tau\} \cup \Lambda \cup \bar{\Lambda}$ , where  $\Lambda$  is a given set of *names*,  $\bar{\Lambda} = \{\bar{a} \mid a \in \Lambda\}$  is the set of *complement names*, and  $\tau$  is a distinguished action. Following Milner [Mil89], the action  $\tau$  will result from the synchronized occurrence of the complementary actions  $a$  and  $\bar{a}$ . We let  $a, b$  range over the set of *visible actions*  $\Lambda \cup \bar{\Lambda}$ . As usual, we postulate that  $\bar{\bar{a}} = a$  for each name  $a \in \Lambda$ . We shall use  $p, q, r$  to range over process terms. The *size* of a term is the number of operation symbols in it. Following standard practice in the literature on CCS and related languages, trailing  $\mathbf{0}$ 's will often be omitted from terms.

The structural operational semantics for the language  $\text{CCS}_H$  given by Hennessy in Sect. 2.1 of [Hen88] is based upon the idea that visible actions have a beginning and an ending. Moreover, for each visible action  $a$ , these distinct events may be observed, and are denoted by  $S(a)$  and  $F(a)$ , respectively. We define

$$E = A \cup \{S(a), F(a) \mid a \in \Lambda \cup \bar{\Lambda}\} .$$

Table 1: SOS Rules for  $S$  ( $\mu \in A$ ,  $a \in \Lambda \cup \bar{\Lambda}$  and  $e \in E$ )

$$\begin{array}{c}
\frac{}{ap \xrightarrow{S(a)} asp} \quad \frac{}{asp \xrightarrow{F(a)} p} \quad \frac{}{\mu p \xrightarrow{\mu} p} \\
\\
\frac{p \xrightarrow{e} s}{p + q \xrightarrow{e} s} \quad \frac{q \xrightarrow{e} s}{p + q \xrightarrow{e} s} \\
\\
\frac{s \xrightarrow{e} s'}{s \mid t \xrightarrow{e} s' \mid t} \quad \frac{t \xrightarrow{e} t'}{s \mid t \xrightarrow{e} s \mid t'} \quad \frac{s \xrightarrow{a} s', t \xrightarrow{\bar{a}} t'}{s \mid t \xrightarrow{\tau} s' \mid t'} \\
\\
\frac{p \xrightarrow{e} s}{p \nmid q \xrightarrow{e} s \mid q} \quad \frac{p \xrightarrow{a} p', q \xrightarrow{\bar{a}} q'}{p \nmid q \xrightarrow{\tau} p' \mid q'}
\end{array}$$

In the terminology of [Hen88], this is the set of *events*, and we shall use  $e$  to range over it. As usual, we write  $E^*$  for the collection of finite sequences of events.

The operational semantics for the language  $\text{CCS}_H$  is given in terms of binary next-state relations  $\xrightarrow{e}$ , one for each event  $e \in E$ . As explained in [Hen88], the relations  $\xrightarrow{e}$  are defined over the set of *states*  $S$ , an extension of  $\text{CCS}_H$  obtained by adding new prefixing operations  $a_S$  ( $a \in \Lambda \cup \bar{\Lambda}$ ) to the signature for  $\text{CCS}_H$ . More formally, the set of states is given by the following grammar:

$$s ::= p \mid asp \mid s \mid s ,$$

where  $p$  ranges over  $\text{CCS}_H$ . Intuitively, a state of the form  $asp$  is one in which the execution of action  $a$  has started, but has not terminated yet. We shall use  $s, t$  to range over the set of states  $S$ .

The Plotkin style rules for the language  $S$  are given in Table 1; comments on these rules may be found in [Hen88, Sect. 2.1].

**Definition 2.1.** For a sequence of events  $\sigma = e_1 \cdots e_k$  ( $k \geq 0$ ), and states  $s, s'$ , we write  $s \xrightarrow{\sigma} s'$  iff there exists a sequence of transitions

$$s = s_0 \xrightarrow{e_1} s_1 \xrightarrow{e_2} \cdots \xrightarrow{e_k} s_k = s' .$$

If  $s \xrightarrow{\sigma} s'$  holds for some state  $s'$ , then  $\sigma$  is a *trace* of  $s$ .

The *depth* of a state  $s$ , written  $\text{depth}(s)$ , is the length of the longest trace it affords.

In this paper, we shall consider the language  $\text{CCS}_H$ , and more generally the set of states  $S$ , modulo split-2 bisimulation equivalence [AH93, GV87, GL95, Hen88]. (The weak variant of this relation is called *t-observational equivalence* by Hennessy in [Hen88]. Later on, this relation has been called *timed equivalence* in [AH93]. Here we adopt the terminology introduced by van Glabbeek and Vaandrager in [GV87].)

**Definition 2.2.** *Split-2 bisimulation equivalence*, denoted by  $\leftrightarrow_{2S}$ , is the largest symmetric relation over  $S$  such that whenever  $s \leftrightarrow_{2S} t$  and  $s \xrightarrow{e} s'$ , then there is a transition  $t \xrightarrow{e} t'$  with  $s' \leftrightarrow_{2S} t'$ .

We shall also sometimes refer to  $\leftrightarrow_{2S}$  as *split-2 bisimilarity*. If  $s \leftrightarrow_{2S} t$ , then we say that  $s$  and  $t$  are *split-2 bisimilar*.

In what follows, we shall mainly be interested in  $\leftrightarrow_{2S}$  as it applies to the language  $\text{CCS}_H$ . The interested reader is referred to [Hen88, Sect. 2.1] for examples of (in)equivalent terms with respect to  $\leftrightarrow_{2S}$ . Here, we limit ourselves to remarking that  $\leftrightarrow_{2S}$  is a non-interleaving equivalence. For example, the reader can easily check that the three terms  $a \mid b$ ,  $a \mid b + ab$  and  $ab + ba$  are pairwise inequivalent.

It is well-known that split-2 bisimulation equivalence is indeed an equivalence relation. Moreover, two split-2 bisimulation equivalent states afford the same finite non-empty set of traces, and have therefore the same depth.

The following result can be shown following standard lines—see, e.g., [AH93].

**Fact 2.3.** *Split-2 bisimilarity is a congruence over the language  $\text{CCS}_H$ . Moreover, for all states  $s, s', t, t'$ , if  $s \leftrightarrow_{2S} s'$  and  $t \leftrightarrow_{2S} t'$ , then  $s \mid t \leftrightarrow_{2S} s' \mid t'$ .*

A standard question a process algebraist would ask at this point, and the one that we shall address in the remainder of this paper, is whether split-2 bisimulation equivalence affords a finite equational axiomatization over the language  $\text{CCS}_H$ . As we showed in [AFIL03], standard bisimulation equivalence is not finitely based over the language  $\text{CCS}_H$ . In particular, we argued there that no finite collection of equations over  $\text{CCS}_H$  that is sound with respect to bisimulation equivalence can prove all of the equations

$$e_n : \quad a\mathbf{0} \not\sim p_n \approx ap_n + \sum_{i=0}^n \tau a^i \quad (n \geq 0) , \quad (2.1)$$

where  $a^0$  denotes  $\mathbf{0}$ ,  $a^{m+1}$  denotes  $aa^m$ , and the terms  $p_n$  are defined thus:

$$p_n = \sum_{i=0}^n \bar{a}a^i \quad (n \geq 0) .$$

Note, however, that none of the equations  $e_n$  holds with respect to  $\leftrightarrow_{2S}$ . In fact, for each  $n \geq 0$ , the transition

$$ap_n + \sum_{i=0}^n \tau a^i \xrightarrow{S(a)} asp_n$$

cannot be matched, modulo  $\leftrightarrow_{2S}$ , by the term  $a\mathbf{0} \not\sim p_n$ . Indeed, the only state reachable from  $a\mathbf{0} \not\sim p_n$  via an  $S(a)$ -labelled transition is  $a_S\mathbf{0} \mid p_n$ . This state is not split-2 bisimilar to  $asp_n$  because it can perform the transition

$$a_S\mathbf{0} \mid p_n \xrightarrow{S(\bar{a})} a_S\mathbf{0} \mid \bar{a}_S\mathbf{0} ,$$

whereas the only initial event  $asp_n$  can embark in is  $F(a)$ . Thus the family of equations on which our proof of the main result from [AFIL03] was based is unsound with respect to split-2 bisimilarity. Indeed, as we shall show in what follows, split-2 bisimilarity affords a finite equational axiomatization over the language  $\text{CCS}_H$ , assuming that the set of actions  $A$  is finite. Hence it is possible to finitely axiomatize split-2 bisimilarity over CCS using a single auxiliary binary operation, viz. Hennessy's merge.

### 3. AN AXIOMATIZATION OF SPLIT-2 BISIMILARITY OVER $\text{CCS}_H$

Let  $\mathcal{E}$  denote the collection of equations in Table 2. In those equations the symbols  $x, y, w, z$  are variables. Equation HM6 is an axiom schema describing one equation per visible action  $a$ . Note that  $\mathcal{E}$  is finite, if so is  $A$ .

Table 2: The Axiom System  $\mathcal{E}$  for  $\text{CCS}_H$  Modulo  $\leftrightarrow_{2S}$ 

A1	$x + y \approx y + x$
A2	$(x + y) + z \approx x + (y + z)$
A3	$x + x \approx x$
A4	$x + \mathbf{0} \approx x$
HM1	$(x + y) \not\mid z \approx x \not\mid z + y \not\mid z$
HM2	$(x \not\mid y) \not\mid z \approx x \not\mid (y \mid z)$
HM3	$x \not\mid \mathbf{0} \approx x$
HM4	$\mathbf{0} \not\mid x \approx \mathbf{0}$
HM5	$(\tau x) \not\mid y \approx \tau(x \mid y)$
HM6	$ax \not\mid ((\bar{a}y \not\mid w) + z) \approx ax \not\mid ((\bar{a}y \not\mid w) + z) + \tau(x \mid y \mid w)$
M	$x \mid y \approx (x \not\mid y) + (y \not\mid x)$

We write  $\mathcal{E} \vdash p \approx q$ , where  $p, q$  are terms in the language  $\text{CCS}_H$  that may possibly contain occurrences of variables, if the equation  $p \approx q$  can be proven from those in  $\mathcal{E}$  using the standard rules of equational logic. For example, using axioms A1, A2, A4, M, HM1, HM2, HM3 and HM4, it is possible to derive the equations:

$$x \mid \mathbf{0} \approx x \quad (3.1)$$

$$\mathbf{0} \mid x \approx x \quad (3.2)$$

$$x \mid y \approx y \mid x \quad \text{and} \quad (3.3)$$

$$(x \mid y) \mid z \approx x \mid (y \mid z) \quad (3.4)$$

that state that, modulo  $\leftrightarrow_{2S}$ , the language  $\text{CCS}_H$  is a commutative monoid with respect to parallel composition with  $\mathbf{0}$  as unit element. (In light of the provability of (3.4), we have taken the liberty of omitting parentheses in the second summand of the term at the right-hand side of equation HM6 in Table 2.) Moreover, it is easy to see that:

**Fact 3.1.** *For each  $\text{CCS}_H$  term  $p$ , if  $p \leftrightarrow_{2S} \mathbf{0}$ , then the equation  $p \approx \mathbf{0}$  is provable using A4, HM4 and M.*

All of the equations in the axiom system  $\mathcal{E}$  may be found in the axiomatization of  $t$ -observational congruence proposed by Hennessy in [Hen88]. However, the abstraction from  $\tau$ -labelled transitions underlying  $t$ -observational congruence renders axiom HM2 above unsound modulo that congruence. (See the discussion in [Ace94, Page 854 and Sect. 3].) Indeed, to the best of our knowledge, it is yet unknown whether  $(t)$ -observational congruence affords a finite equational axiomatization over  $\text{CCS}$ , with or without Hennessy's merge.

Our aim, in the remainder of this note, will be to show that, in the presence of a finite collection of actions  $A$ , split-2 bisimilarity is finitely axiomatizable over the language  $\text{CCS}_H$ . This is the import of the following:

**Theorem 3.2.** *For all  $\text{CCS}_H$  terms  $p, q$  not containing occurrences of variables,  $p \leftrightarrow_{2S} q$  if, and only if,  $\mathcal{E} \vdash p \approx q$ .*

We now proceed to prove the above theorem by establishing separately that the axiom system  $\mathcal{E}$  is sound and complete.

**Proposition 3.3** (Soundness). *For all  $CCS_H$  terms  $p, q$ , if  $\mathcal{E} \vdash p \approx q$ , then  $p \xleftrightarrow{2S} q$ .*

*Proof.* Since  $\xleftrightarrow{2S}$  is a congruence over the language  $CCS_H$  (Fact 2.3), it suffices only to check that each of the equations in  $\mathcal{E}$  is sound. The verification is tedious, but not hard, and we omit the details.  $\square$

**Remark 3.4.** For later use in the proof of Proposition 3.11, we note that equations (3.1)–(3.4) also hold modulo  $\xleftrightarrow{2S}$  when the variables  $x, y, z$  are allowed to range over the set of states  $S$ .

The proof of the completeness of the equations in  $\mathcal{E}$  with respect to  $\xleftrightarrow{2S}$  follows the general outline of that of [Hen88, Theorem 2.1.2]. As usual, we rely upon the existence of normal forms for  $CCS_H$  terms. In the remainder of this paper, process terms are considered modulo associativity and commutativity of  $+$ . In other words, we do not distinguish  $p + q$  and  $q + p$ , nor  $(p + q) + r$  and  $p + (q + r)$ . This is justified because, as previously observed, split-2 bisimulation equivalence satisfies axioms A1, A2 in Table 2. In what follows, the symbol  $=$  will denote equality modulo axioms A1, A2. We use a *summation*  $\sum_{i \in \{1, \dots, k\}} p_i$  to denote  $p_1 + \dots + p_k$ , where the empty sum represents  $\mathbf{0}$ .

**Definition 3.5.** The set  $NF$  of *normal forms* is the least subset of  $CCS_H$  such that

$$\sum_{i \in I} (a_i p_i \mid p'_i) + \sum_{j \in J} \tau q_j \in NF \ ,$$

where  $I, J$  are finite index sets, if the following conditions hold:

- (1) the terms  $p_i, p'_i$  ( $i \in I$ ) and  $q_j$  ( $j \in J$ ) are contained in  $NF$  and
- (2) if  $a_i p_i \mid p'_i \xrightarrow{\tau} q$  for some  $q$ , then  $q = q_j$  for some  $j \in J$ .

**Proposition 3.6** (Normalization). *For each  $CCS_H$  term  $p$ , there is a term  $\hat{p} \in NF$  such that  $\mathcal{E} \vdash p \approx \hat{p}$ .*

*Proof.* Define the relation  $\sqsubset$  on  $CCS_H$  terms thus:

- $p \sqsubset q$  if, and only if,
  - $depth(p) < depth(q)$  or
  - $depth(p) = depth(q)$  and the size of  $p$  is smaller than that of  $q$ .

Note that  $\sqsubset$  is a well-founded relation, so we may use  $\sqsubset$ -induction. The remainder of the proof consists of a case analysis on the syntactic form of  $p$ .

We only provide the details for the case  $p = q \mid r$ . (The cases  $p = \mathbf{0}$ ,  $p = q + r$  and  $p = \mu q$  are trivial—the last owing to the fact that  $\mu q \approx \mu q \mid \mathbf{0}$  is an instance of axiom HM3—, and the case  $p = q \mid r$  follows from the case that is treated in detail using axiom M.)

Assume therefore that  $p = q \mid r$ . Then  $depth(q) \leq depth(p)$  and the size of  $q$  is smaller than that of  $p$ , so  $q \sqsubset p$ . Hence, by the induction hypothesis there exists  $\hat{q} \in NF$  such that  $\mathcal{E} \vdash q \approx \hat{q}$ , say

$$\hat{q} = \sum_{i \in I} (a_i q_i \mid q'_i) + \sum_{j \in J} \tau q''_j \ .$$

By axioms HM1, HM2, HM4 and HM5 it follows that

$$p \approx \sum_{i \in I} a_i q_i \mid (q'_i \mid r) + \sum_{j \in J} \tau (q''_j \mid r) \ .$$



Since  $\text{depth}(q'_i), \text{depth}(q''_j) < \text{depth}(\hat{q}) = \text{depth}(q)$  for each  $i \in I$  and  $j \in J$ , it follows that

$$\text{depth}(q'_i | r), \text{depth}(q''_j | r) < \text{depth}(\hat{q} | r) = \text{depth}(q | r) = \text{depth}(p) ,$$

and hence  $q'_i | r \sqsubset p$  and  $q''_j | r \sqsubset p$ . By the induction hypothesis there are normal forms  $\widehat{q'_i | r}, \widehat{q''_j | r}$  such that  $\mathcal{E} \vdash q'_i | r \approx \widehat{q'_i | r}, q''_j | r \approx \widehat{q''_j | r}$ . So  $\mathcal{E}$  proves the equation

$$p \approx \sum_{i \in I} a_i q_i | (\widehat{q'_i | r}) + \sum_{j \in J} \tau(\widehat{q''_j | r}) . \quad (3.5)$$

Finally, using equation HM6, it is now a simple matter to add summands to the right-hand side of the above equation in order to meet requirement 2 in Definition 3.5. In fact, let  $i \in I$  and

$$\widehat{q'_i | r} = \sum_{h \in H} (a_h r_h | r'_h) + \sum_{k \in K} \tau r''_k .$$

Using A4, we have that

$$\widehat{q'_i | r} \approx \sum_{h \in H, a_h = \bar{a}_i} (a_h r_h | r'_h) + \sum_{h \in H, a_h \neq \bar{a}_i} (a_h r_h | r'_h) + \sum_{k \in K} \tau r''_k$$

is provable from  $\mathcal{E}$ . Then, using HM6 and the induction hypothesis repeatedly, we can prove the equation

$$a_i q_i | (\widehat{q'_i | r}) \approx a_i q_i | (\widehat{q'_i | r}) + \sum_{h \in H, a_h = \bar{a}_i} \tau(q_i | r_h | r'_h) .$$

Using this equation as a rewrite rule from left to right in (3.5) for each  $i \in I$  produces a term meeting requirement 2 in Definition 3.5 that is the desired normal form for  $p = q | r$ .  $\square$

The key to the proof of the promised completeness theorem is an important cancellation result that has its roots in one proven by Hennessy for his t-observational equivalence in [Hen88].

**Theorem 3.7.** *Let  $p, p', q, q'$  be  $\text{CCS}_H$  terms, and let  $a$  be a visible action. Assume that*

$$a_S p | p' \xleftrightarrow{2S} a_S q | q' .$$

*Then  $p \xleftrightarrow{2S} q$  and  $p' \xleftrightarrow{2S} q'$ .*

For the moment, we postpone the proof of this result, and use it to establish the following statement, to the effect that the axiom system  $\mathcal{E}$  is complete with respect to  $\xleftrightarrow{2S}$  over  $\text{CCS}_H$ .

**Theorem 3.8** (Completeness). *Let  $p, q$  be  $\text{CCS}_H$  terms such that  $p \xleftrightarrow{2S} q$ . Then  $\mathcal{E} \vdash p \approx q$ .*

*Proof.* By induction on the depth of  $p$  and  $q$ . (Recall that, since  $p \xleftrightarrow{2S} q$ , the terms  $p$  and  $q$  have the same depth.) In light of Proposition 3.6, we may assume without loss of generality that  $p$  and  $q$  are contained in NF. Let

$$\begin{aligned} p &= \sum_{i \in I} (a_i p_i | p'_i) + \sum_{j \in J} \tau p''_j \quad \text{and} \\ q &= \sum_{h \in H} (b_h q_h | q'_h) + \sum_{k \in K} \tau q''_k . \end{aligned}$$

We prove that  $\mathcal{E} \vdash p \approx p + q$ , from which the statement of the theorem follows by symmetry and transitivity. To this end, we argue that each summand of  $q$  can be absorbed into  $p$  using the equations in  $\mathcal{E}$ , i.e., that

- (1)  $\mathcal{E} \vdash p \approx p + \tau q_k''$  for each  $k \in K$ , and
- (2)  $\mathcal{E} \vdash p \approx p + (b_h q_h \mid q_h')$  for each  $h \in H$ .

We prove these two statements in turn.

- **PROOF OF STATEMENT 1.** Let  $k \in K$ . Then  $q \xrightarrow{\tau} q_k''$ . Since  $p \xleftrightarrow{2S} q$ , there is a term  $r$  such that  $p \xrightarrow{\tau} r$  and  $r \xleftrightarrow{2S} q_k''$ . Since  $p \in \text{NF}$ , condition 2 in Definition 3.5 yields that  $r = p_j''$  for some  $j \in J$ . The induction hypothesis together with closure with respect to  $\tau$ -prefixing now yields that

$$\mathcal{E} \vdash \tau p_j'' \approx \tau q_k''.$$

Therefore, using A1–A3, we have that

$$\mathcal{E} \vdash p \approx p + \tau p_j'' \approx p + \tau q_k'' ,$$

which was to be shown.

- **PROOF OF STATEMENT 2.** Let  $h \in H$ . Then  $q \xrightarrow{S(b_h)} b_h q_h \mid q_h'$ . Since  $p \xleftrightarrow{2S} q$ , there is a state  $s$  such that  $p \xrightarrow{S(b_h)} s$  and  $s \xleftrightarrow{2S} b_h q_h \mid q_h'$ . Because of the form of  $p$ , it follows that  $s = a_i s p_i \mid p_i'$  for some  $i \in I$  such that  $a_i = b_h$ . By Theorem 3.7, we have that

$$p_i \xleftrightarrow{2S} q_h \text{ and } p_i' \xleftrightarrow{2S} q_h' .$$

Since the depth of all of these terms is smaller than that of  $p$ , we may apply the induction hypothesis twice to obtain that

$$\mathcal{E} \vdash p_i \approx q_h \text{ and } \mathcal{E} \vdash p_i' \approx q_h' .$$

Therefore, using A1–A3 and  $a_i = b_h$ , we have that

$$\mathcal{E} \vdash p \approx p + (a_i p_i \mid p_i') \approx p + (b_h q_h \mid q_h') ,$$

which was to be shown.

The proof of the theorem is now complete.  $\square$

To finish the proof of the completeness theorem, and therefore of Theorem 3.2, we are left to show Theorem 3.7. Our proof of that result relies on a unique decomposition property with respect to parallel composition for states modulo  $\xleftrightarrow{2S}$ . In order to formulate this decomposition property, we shall make use of some notions from [MM93, Mol89]. These we now proceed to introduce for the sake of completeness and readability.

**Definition 3.9.** A state  $s$  is *irreducible* if  $s \xleftrightarrow{2S} s_1 \mid s_2$  implies  $s_1 \xleftrightarrow{2S} \mathbf{0}$  or  $s_2 \xleftrightarrow{2S} \mathbf{0}$ , for all states  $s_1, s_2$ .

We say that  $s$  is *prime* if it is irreducible and is not split-2 bisimilar to  $\mathbf{0}$ .

For example, each state  $s$  of depth 1 is prime because every state of the form  $s_1 \mid s_2$ , where  $s_1$  and  $s_2$  are not split-2 bisimilar to  $\mathbf{0}$ , has depth at least 2, and thus cannot be split-2 bisimilar to  $s$ .

**Fact 3.10.** *The state  $a s p$  is prime, for each  $\text{CCS}_H$  term  $p$  and action  $a$ .*

*Proof.* Since  $a_{SP}$  is not split-2 bisimilar to  $\mathbf{0}$ , it suffices only to show that it is irreducible. To this end, assume, towards a contradiction, that  $a_{SP} \Leftrightarrow_{2S} s_1 \mid s_2$  for some states  $s_1, s_2$  that are not split-2 bisimilar to  $\mathbf{0}$ . Then, since  $a_{SP} \Leftrightarrow_{2S} s_1 \mid s_2$ , we have that  $s_1 \xrightarrow{F(a)} s'_1$  and  $s_2 \xrightarrow{F(a)} s'_2$ , for some  $s'_1, s'_2$ . But then it follows that

$$s_1 \mid s_2 \xrightarrow{F(a)} s'_1 \mid s_2 \xrightarrow{F(a)} s'_1 \mid s'_2 ,$$

whereas the term  $a_{SP}$  cannot perform two subsequent  $F(a)$ -transitions. We may therefore conclude that such states  $s_1$  and  $s_2$  cannot exist, and hence that the term  $a_{SP}$  is irreducible, which was to be shown.  $\square$

The following result is the counterpart for the language  $\text{CCS}_H$  of the unique decomposition theorems presented for various languages in, e.g., [AH93, Lut03, MM93, Mol89].

**Proposition 3.11.** *Each state is split-2 bisimilar to a parallel composition of primes, uniquely determined up to split-2 bisimilarity and the order of the primes. (We adopt the convention that  $\mathbf{0}$  denotes the empty parallel composition.)*

*Proof.* We shall obtain this result as a consequence of a general unique decomposition result, obtained by the fourth author in [Lut03].

Let  $[S]$  denote the set of states modulo split-2 bisimilarity, and, for a state  $s \in S$ , denote by  $[s]$  the equivalence class in  $[S]$  that contains  $s$ . By Fact 2.3 we can define on  $[S]$  a binary operation  $\mid$  by

$$[s] \mid [t] = [s \mid t] .$$

By Remark 3.4, the set  $[S]$  with the binary operation  $\mid$  and the distinguished element  $[\mathbf{0}]$  is a commutative monoid.

Next, we define on  $[S]$  a partial order  $\preceq$  by

$$[s'] \preceq [s] \text{ iff there exist } s'' \in S \text{ and } \sigma \in E^* \text{ such that } s \xrightarrow{\sigma} s'' \Leftrightarrow_{2S} s' .$$

Note that  $\preceq$  is indeed a partial order (to establish antisymmetry use that transitions decrease depth, and that split-2 bisimilar states have the same depth).

For each state  $s$ , there are a sequence of events  $\sigma$  and a state  $s'$  such that

$$s \xrightarrow{\sigma} s' \Leftrightarrow_{2S} \mathbf{0} .$$

So  $[\mathbf{0}]$  is the least element of  $[S]$  with respect to  $\preceq$ . Furthermore, if  $[s'] \preceq [s]$ , then  $s \xrightarrow{\sigma} s'' \Leftrightarrow_{2S} s'$ , for some  $\sigma \in E^*$  and state  $s''$ . So, using the SOS rules for  $S$  and Fact 2.3, it follows that

$$s \mid t \xrightarrow{\sigma} s'' \mid t \Leftrightarrow_{2S} s' \mid t ,$$

and hence

$$[s'] \mid [t] = [s' \mid t] \preceq [s \mid t] = [s] \mid [t] .$$

Thereby, we have now established that  $[S]$  with  $\mid$ ,  $[\mathbf{0}]$  and  $\preceq$  is a positively ordered commutative monoid in the sense of [Lut03].

From the SOS rules for  $S$  it easily follows that this positively ordered commutative monoid is *precompositional* (see [Lut03]), i.e., that

$$\text{if } [s] \preceq [s_1] \mid [s_2], \text{ then there are } [s'_1] \preceq [s_1], [s'_2] \preceq [s_2] \text{ s.t. } [s] = [s'_1] \mid [s'_2] .$$

Consider the mapping  $|\cdot| : [S] \rightarrow \mathbf{N}$  into the positively ordered monoid of natural numbers with addition, 0 and the standard less-than-or-equal relation, defined by

$$[s] \mapsto \text{depth}(s) .$$

It is straightforward to verify that  $|\cdot|$  is a *stratification* (see [Lut03]), i.e., that

- (i)  $||[s]| \mid [t]| = |[s]| + |[t]|$ ; and
- (ii) if  $[s] \prec [t]$ , then  $|[s]| < |[t]|$ .

We conclude that  $[S]$  with  $|\cdot|$ ,  $[0]$  and  $\prec$  is a stratified and precompositional positively ordered commutative monoid, and hence, by Theorem 13 in [Lut03], it has unique decomposition. This completes the proof of the proposition.  $\square$

Using the above unique decomposition result, we are now in a position to complete the proof of Theorem 3.7.

*Proof of Theorem 3.7:* Assume that  $a_{SP} \mid p' \xleftrightarrow{2S} a_{SQ} \mid q'$ . Using Proposition 3.11, we have that  $p'$  and  $q'$  can be expressed uniquely as parallel compositions of primes. Say that

$$\begin{aligned} p' &\xleftrightarrow{2S} p_1 \mid p_2 \mid \cdots \mid p_m \quad \text{and} \\ q' &\xleftrightarrow{2S} q_1 \mid q_2 \mid \cdots \mid q_n \end{aligned}$$

for some  $m, n \geq 0$  and primes  $p_i$  ( $1 \leq i \leq m$ ) and  $q_j$  ( $1 \leq j \leq n$ ) in the language  $\text{CCS}_H$ . Since  $a_{SP}$  and  $a_{SQ}$  are prime (Fact 3.10) and  $\xleftrightarrow{2S}$  is a congruence (Fact 2.3), the unique prime decompositions of  $a_{SP} \mid p'$  and  $a_{SQ} \mid q'$  given by Proposition 3.11 are

$$\begin{aligned} a_{SP} \mid p &\xleftrightarrow{2S} a_{SP} \mid p_1 \mid p_2 \mid \cdots \mid p_m \quad \text{and} \\ a_{SQ} \mid q' &\xleftrightarrow{2S} a_{SQ} \mid q_1 \mid q_2 \mid \cdots \mid q_n, \end{aligned}$$

respectively. In light of our assumption that  $a_{SP} \mid p' \xleftrightarrow{2S} a_{SQ} \mid q'$ , these two prime decompositions coincide by Proposition 3.11. Hence, as for each  $1 \leq j \leq n$

$$a_{SP} \not\xleftrightarrow{2S} q_j,$$

we have that

- (1)  $a_{SP} \xleftrightarrow{2S} a_{SQ}$ ,
- (2)  $m = n$  and, without loss of generality,
- (3)  $p_i \xleftrightarrow{2S} q_i$  for each  $1 \leq i \leq m$ .

It is now immediate to see that  $p \xleftrightarrow{2S} q$  and  $p' \xleftrightarrow{2S} q'$ , which was to be shown.  $\square$

#### ACKNOWLEDGEMENTS

We thank the referees for suggestions that led to improvements in the presentation of the paper. The work reported in this paper was carried out while Luca Aceto was on leave at Reykjavík University, Wan Fokkink was at CWI, and Anna Ingólfssdóttir was at deCODE Genetics. They thank these institutions for their hospitality and excellent working conditions. Luca Aceto's work was partially supported by the Statens Naturvidenskabelige Forskningsråd (Danish Natural Science Research Council), project "The Equational Logic of Parallel Processes", nr. 21-03-0342.

#### REFERENCES

- [Ace94] Luca Aceto. On "Axiomatising finite concurrent processes". *SIAM Journal on Computing*, 23(4):852–863, 1994.
- [Ace03] Luca Aceto. Some of my favourite results in classic process algebra. In Vladimiro Sassone, editor, *Bulletin of the European Association for Theoretical Computer Science*, volume 81, pages 89–108. 2003.
- [AFIL03] Luca Aceto, Wan Fokkink, Anna Ingólfssdóttir, and Bas Luttik. CCS with Hennessy's merge has no finite equational axiomatization. Research report RS-03-34, BRICS, November 2003. To appear in *Theoretical Computer Science*.

- [AH93] L. Aceto and M. Hennessy. Towards action refinement in process algebras. *Information and Computation*, 103(2):204–269, April 1993.
- [Bae04] Jos C.M. Baeten. A brief history of process algebra. Report CSR 04-02, Eindhoven University of Technology, 2004.
- [BK84] J.A. Bergstra and Jan Willem Klop. Process algebra for synchronous communication. *Information and Control*, 60(1/3):109–137, 1984.
- [BW90] Jos C.M. Baeten and P. Weijland. *Process Algebra*. Cambridge Tracts in Theoretical Computer Science 18. Cambridge University Press, 1990.
- [GL95] Roberto Gorrieri and Cosimo Laneve. Split and ST bisimulation semantics. *Information and Computation*, 118(2):272–288, 1995.
- [GV87] R. van Glabbeek and F. Vaandrager. Petri net models for algebraic theories of concurrency. In J. de Bakker, A.J. Nijman, and P.C. Treleaven, editors, *Proceedings PARLE conference*, Eindhoven, Vol. II (*Parallel Languages*), volume 259 of *Lecture Notes in Computer Science*, pages 224–242. Springer-Verlag, 1987.
- [Hen88] M. Hennessy. Axiomatising finite concurrent processes. *SIAM Journal on Computing*, 17(5):997–1017, 1988.
- [HM85] M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the ACM*, 32(1):137–161, 1985.
- [Lut03] Bas Luttik. A unique decomposition theorem for ordered monoids with applications in process theory. In Branislav Rovan and Peter Vojtás, editors, *Proceedings of Mathematical Foundations of Computer Science 2003, 28th International Symposium, MFCS 2003, Bratislava, Slovakia, August 25–29, 2003*, volume 2747 of *Lecture Notes in Computer Science*, pages 562–571. Springer-Verlag, 2003.
- [Mil89] R. Milner. *Communication and Concurrency*. Prentice-Hall International, Englewood Cliffs, 1989.
- [MM93] R. Milner and F. Moller. Unique decomposition of processes (note). *Theoretical Computer Science*, 107(2):357–363, 1993.
- [Mol89] F. Moller. *Axioms for Concurrency*. PhD thesis, Department of Computer Science, University of Edinburgh, July 1989. Report CST-59-89. Also published as ECS-LFCS-89-84.
- [Mol90a] F. Moller. The importance of the left merge operator in process algebras. In M. Paterson, editor, *Proceedings 17<sup>th</sup> ICALP*, Warwick, volume 443 of *Lecture Notes in Computer Science*, pages 752–764. Springer-Verlag, July 1990.
- [Mol90b] F. Moller. The nonexistence of finite axiomatisations for CCS congruences. In *Proceedings 5<sup>th</sup> Annual Symposium on Logic in Computer Science*, Philadelphia, USA, pages 142–153. IEEE Computer Society Press, 1990.
- [Par81] D.M.R. Park. Concurrency and automata on infinite sequences. In P. Deussen, editor, *5<sup>th</sup> GI Conference*, Karlsruhe, Germany, volume 104 of *Lecture Notes in Computer Science*, pages 167–183. Springer-Verlag, 1981.